RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PART3-R03

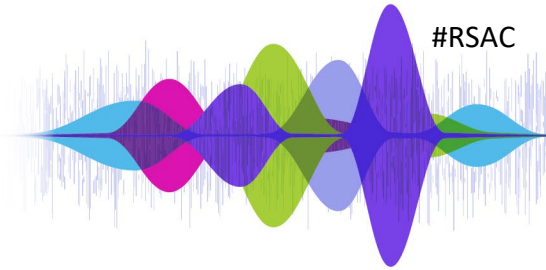
Software Supply Chain Security, AI, and Regulation

Mitch Ashley

VP Practice Lead, DevOps and Application Development
The Futurum Group
https://futurumgroup.com

Tyler Warden

Senior Vice President, Product
Sonatype
https://sonatype.com



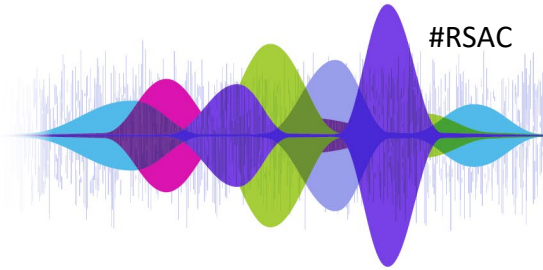
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Software Supply Chain Security, AI, and Regulation



Examine how AI adoption and evolving regulations reshape the software supply chain security landscape by analyzing emerging trends, compliance requirements, and AI's dual role as both risk and solution.

We will discuss insights and practical steps for security teams adapting to these modern, interconnected challenges.

Today's Speakers

Mitch Ashley

VP Practice Lead
DevOps and Application Development

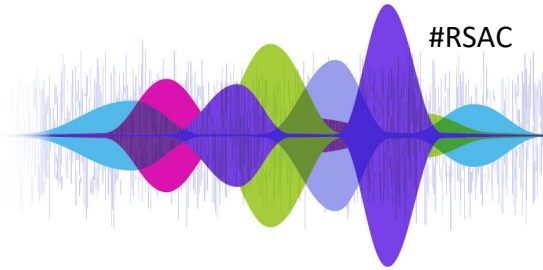
Futurum

Tyler Warren

Senior Vice President
Product

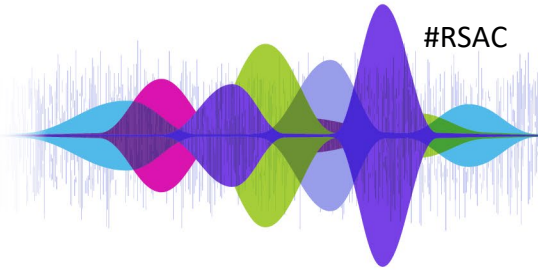
Sonatype

Today's Topics



- Research
  - CEO and CIO Perspectives
  - Current and Future Impact of AI Across Software Organizations
  - AI Critical To Development, Platforms, and Production
  - State of Software Security
- Discussion
  - AI Models/Agents & The Supply Chain
  - New Threat Landscape
  - Regulatory Impact

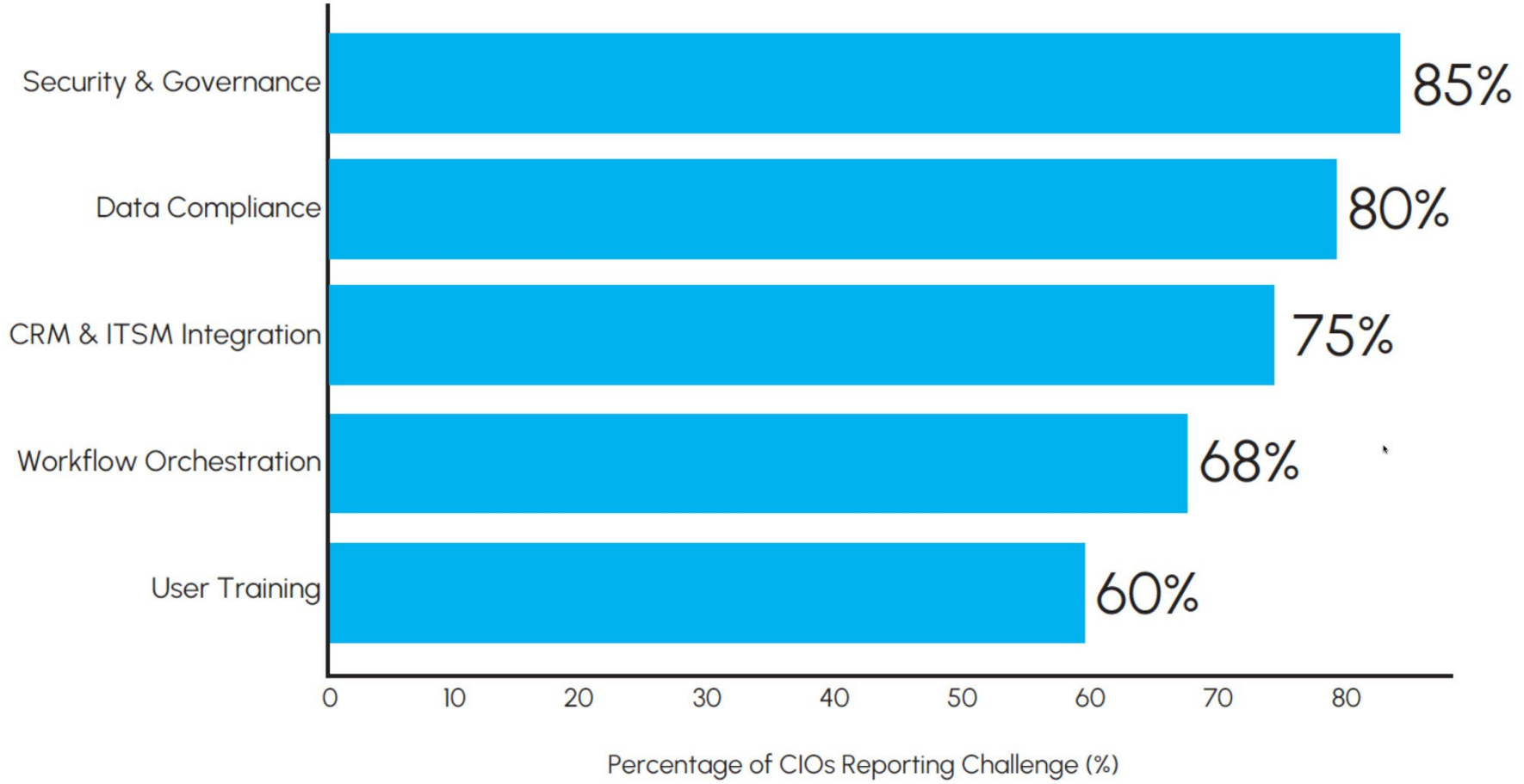
CEOs Are Placing Bets – AI To Deliver



A 2025 study by Futurum and Kearney revealed that **59% of firms are actively investing in "foundational" AI pilots** to build up data readiness and upskill teams, aiming to be prepared when market pressures inevitably rise. Moreover, **89% of surveyed CEOs acknowledge the strategic importance of leveraging AI** for business transformation, yet **only one in four CEOs feel fully prepared** to integrate it across their organizations.

Source: DevOps Future Is AI and Kubernetes, Futurum Intelligence, 2024

CIO Insights: Agentic AI Platforms Challenges In Enterprises

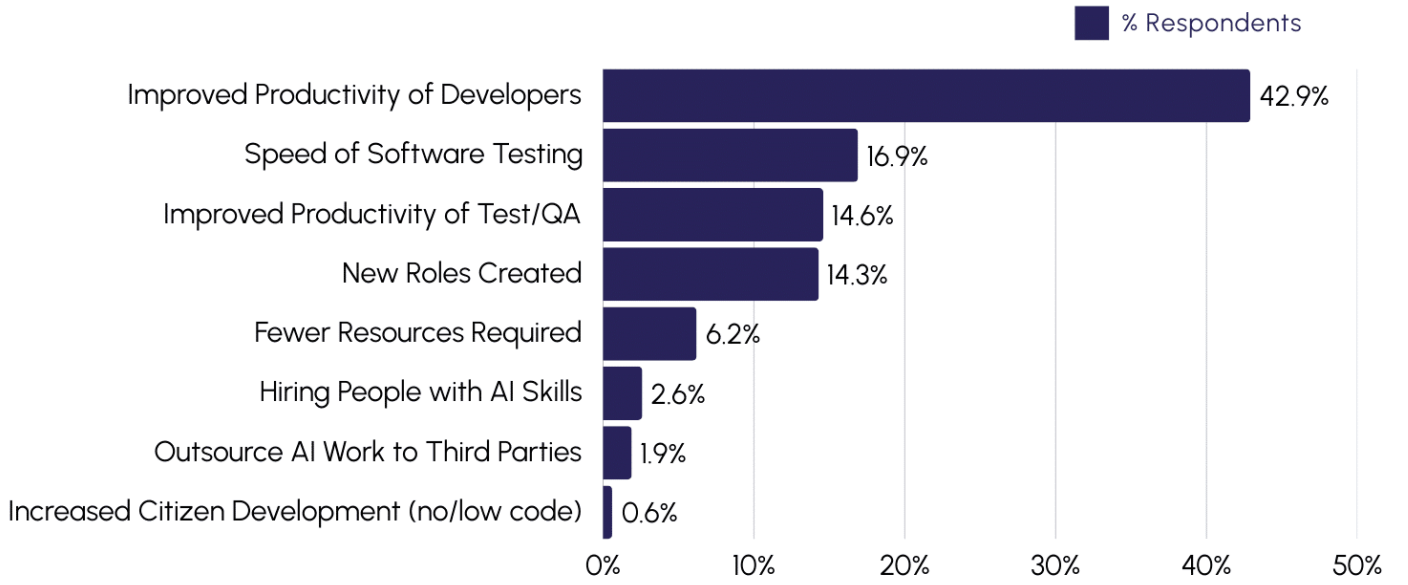


Source: Futurum CIO Insights, Q1 2025 CIO Survey

AI Is Already Changing Roles

Futurum | How AI is Changing Job Functions in Organizations

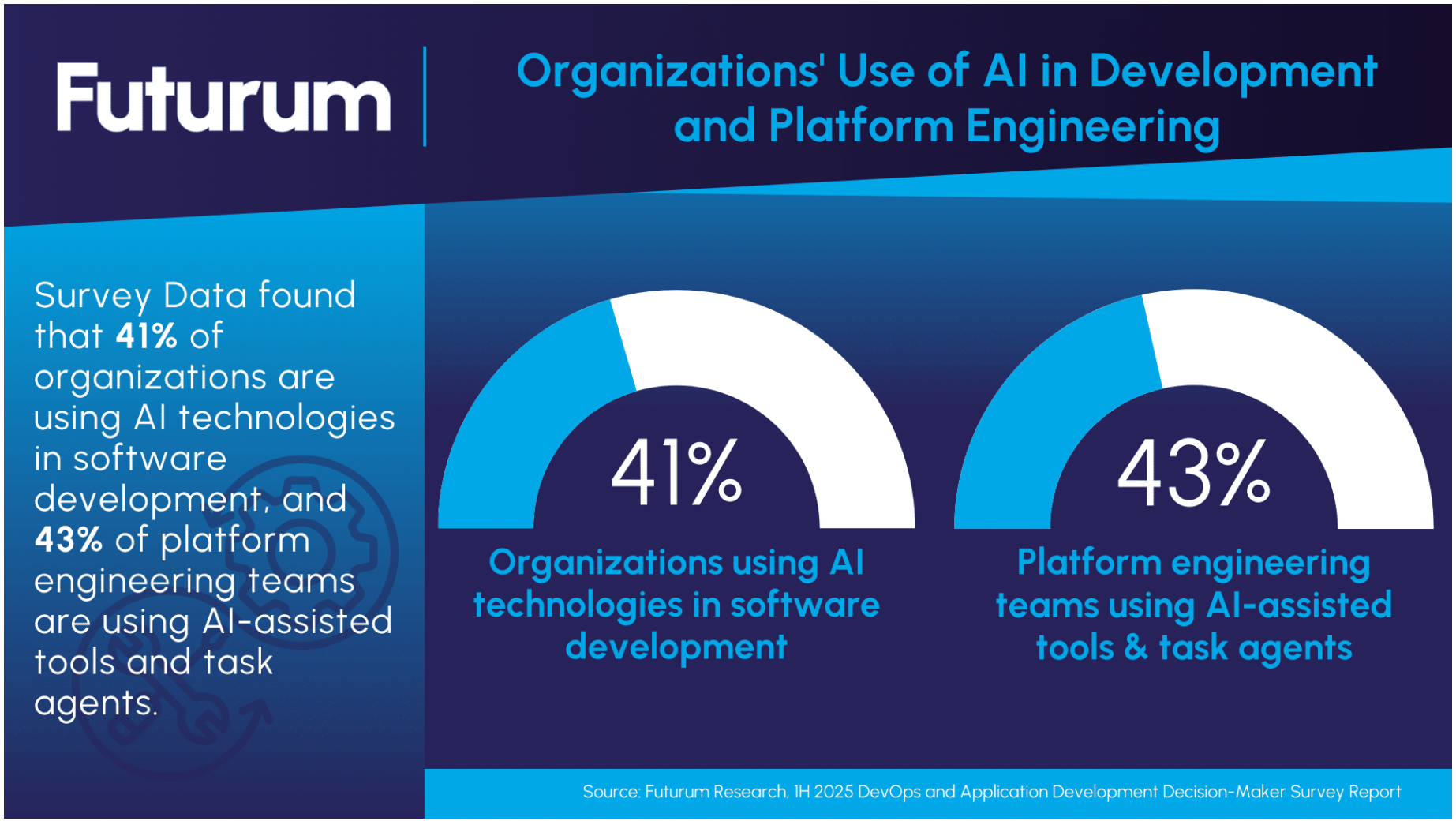
Survey data shows **development organizations emphasize developer productivity across the sum of their work and tasks**, much more than just generating more code faster.



Question: How is AI changing job functions in your organization? (n=308)

Source: Futurum Research, 1H 2025 DevOps and Application Development Decision-Maker Survey Report

Using AI Today


Futurum
Organizations' Use of AI in Development and Platform Engineering
Survey Data found that 41% of organizations are using AI technologies in software development, and 43% of platform engineering teams are using AI-assisted tools and task agents.
41%
Organizations using AI technologies in software development
43%
Platform engineering teams using AI-assisted tools & task agents
Source: Futurum Research, 1H 2025 DevOps and Application Development Decision-Maker Survey Report

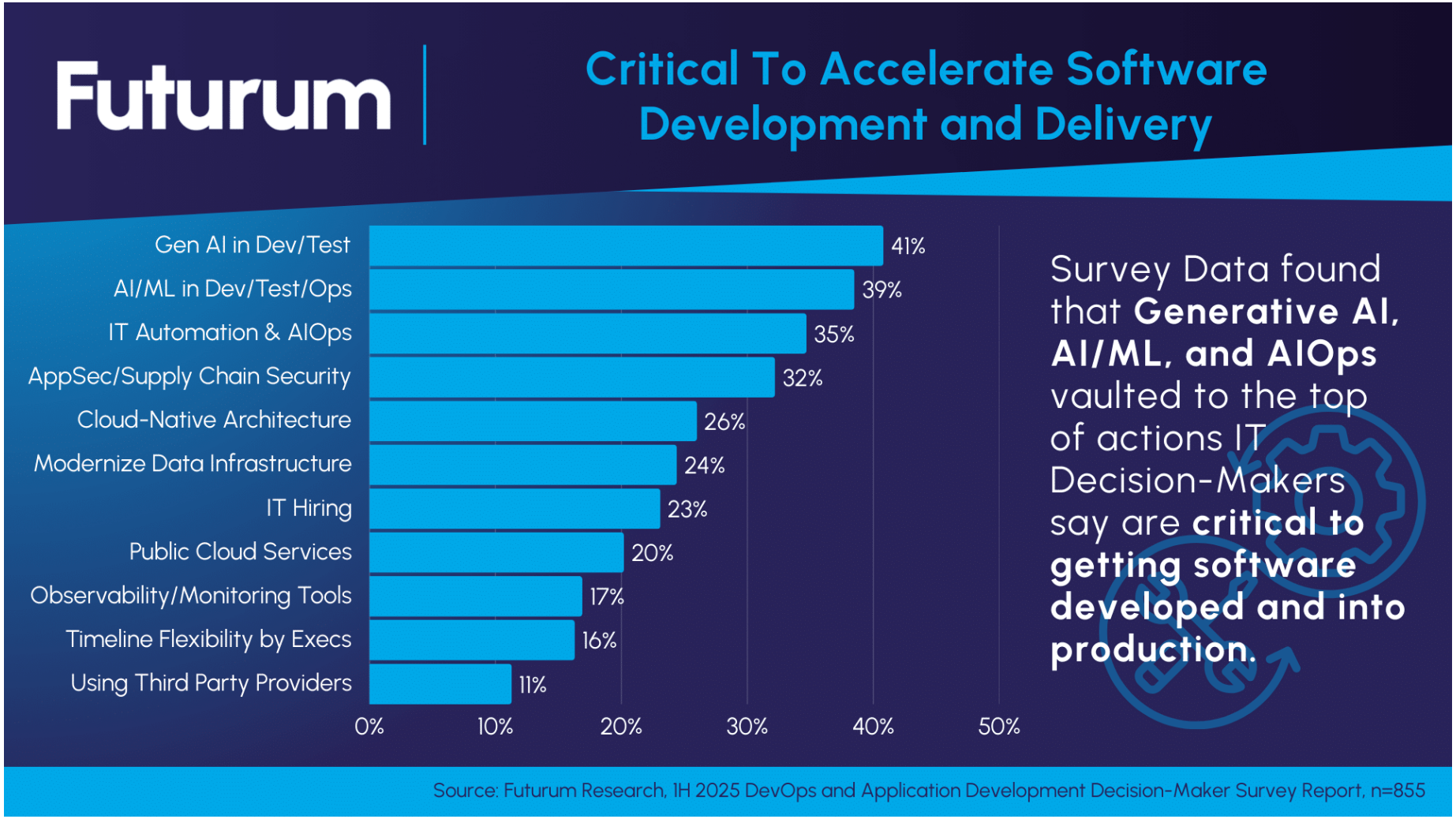
Applying AI To Secure Codebases

During Q3-Q4 2024, LLMs and specialized smaller language models (SLMs) emerged in the market as powerful tools in DevOps and security.

These models **analyze codebases to identify and patch vulnerabilities, suggest secure configurations**, and recommend software upgrades. In DevSecOps, they will play an increasingly important role in **reducing vulnerabilities and maintaining compliance**, aiding developers and security teams in managing and remediation of security vulnerabilities.

Source: DevOps Future Is AI and Kubernetes, Futurum Intelligence, 2024

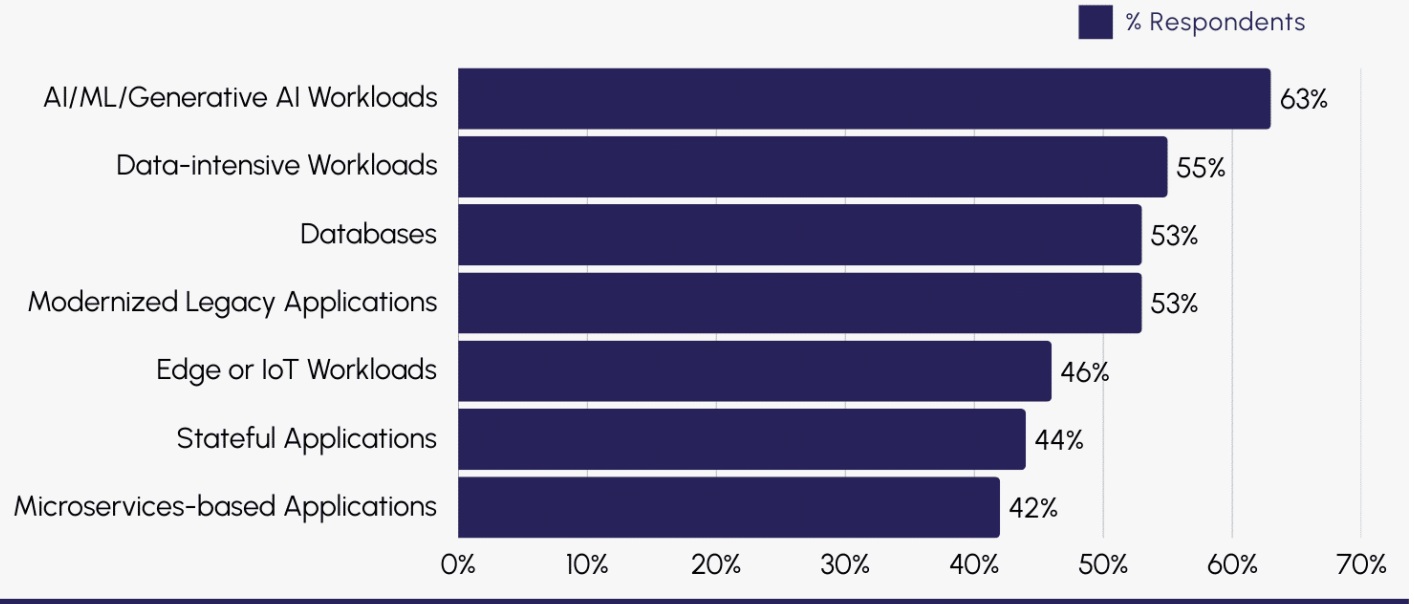
AI Critical To Development and Delivery


Futurum
Critical To Accelerate Software Development and Delivery
Gen AI in Dev/Test 41%
AI/ML in Dev/Test/Ops 39%
IT Automation & AIOps 35%
AppSec/Supply Chain Security 32%
Cloud-Native Architecture 26%
Modernize Data Infrastructure 24%
IT Hiring 23%
Public Cloud Services 20%
Observability/Monitoring Tools 17%
Timeline Flexibility by Execs 16%
Using Third Party Providers 11%
0% 10% 20% 30% 40% 50%
Survey Data found that Generative AI, AI/ML, and AIOps vaulted to the top of actions IT Decision-Makers say are critical to getting software developed and into production.
Source: Futurum Research, 1H 2025 DevOps and Application Development Decision-Maker Survey Report, n=855

AI Workloads

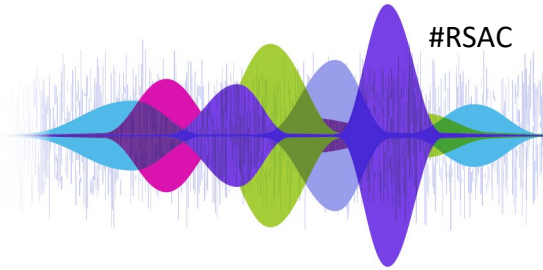
Futurum | Workload Types Deployed on Kubernetes

Survey data shows **AI/ML/Generative AI, data, and modernized legacy applications** at the top of workload types deployed on Kubernetes today.



Source: Futurum Research, 1H 2025 DevOps and Application Development Decision-Maker Survey Report

Software Security: 12-18 Month Outlook



Organizations increasingly recognize the importance of software security and are allocating budgets to address it.

Research by Futurum conducted in early 2025 shows that **27% to 35% of organizations plan to significantly increase** spending on application security over the next 12-18 months.

Similarly, **41% to 45% of organizations plan to moderately increase their software security spending** over the same time period.

Source: Securing Your Software Supply Chain: A Boardroom and C-Suite Imperative, Futurum Intelligence, 2025

Software Security Priorities Outlook

	Software Bill of Materials (SBOM)	Software Composition Analysis (SCA)	Secure Code and Library Repository	Secure Open-source Solutions	DevOps Toolchain Security	App Security Incident Response
Significant Increase	30%	27%	31%	32%	35%	34%
Moderate Increase	42%	41%	44%	42%	42%	45%

Source: Securing Your Software Supply Chain: A Boardroom and C-Suite Imperative, Futurum Intelligence, 2025

Open Source – By The Numbers

OPEN SOURCE SCALE AND CONSUMPTION BEHAVIORS BY THE NUMBERS

512,847
malicious packages discovered since November 2023

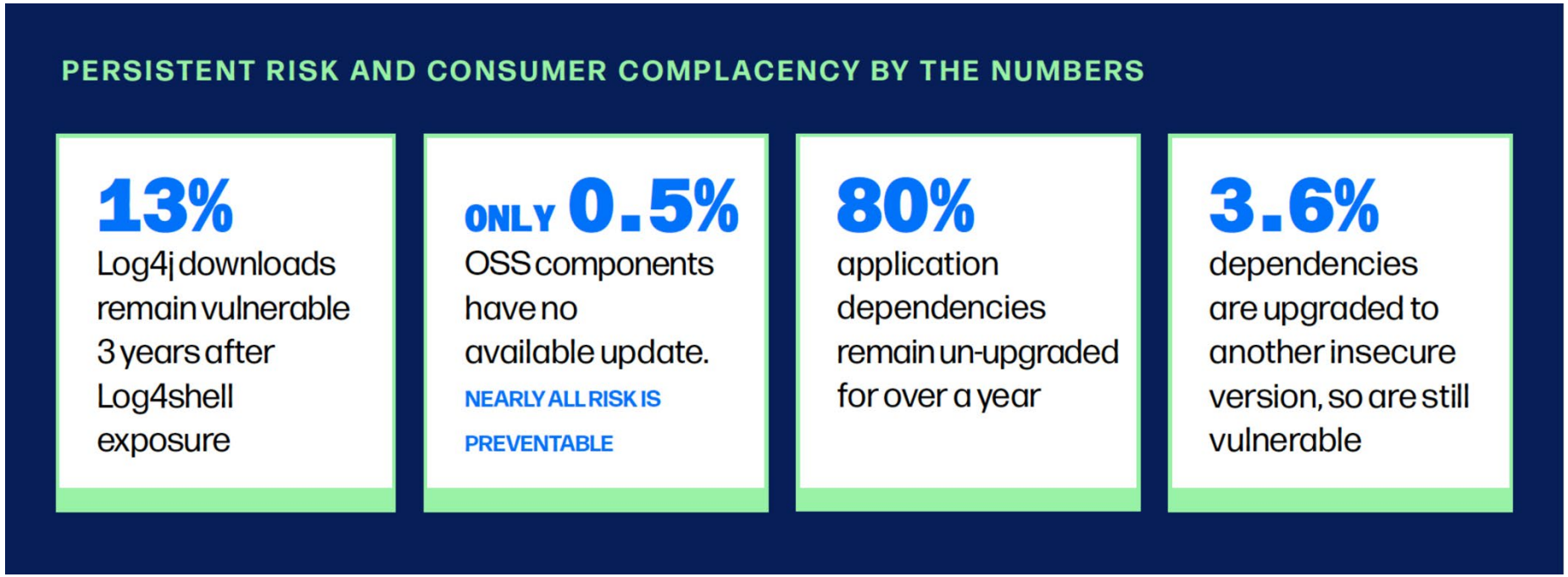
156%
YoY growth of malicious packages

4.5 TRILLION
JavaScript (npm) requests, 70% YoY growth

530 BILLION
Python (PyPI) package requests, 80% YoY increase LARGELY DRIVEN BY AI & CLOUD

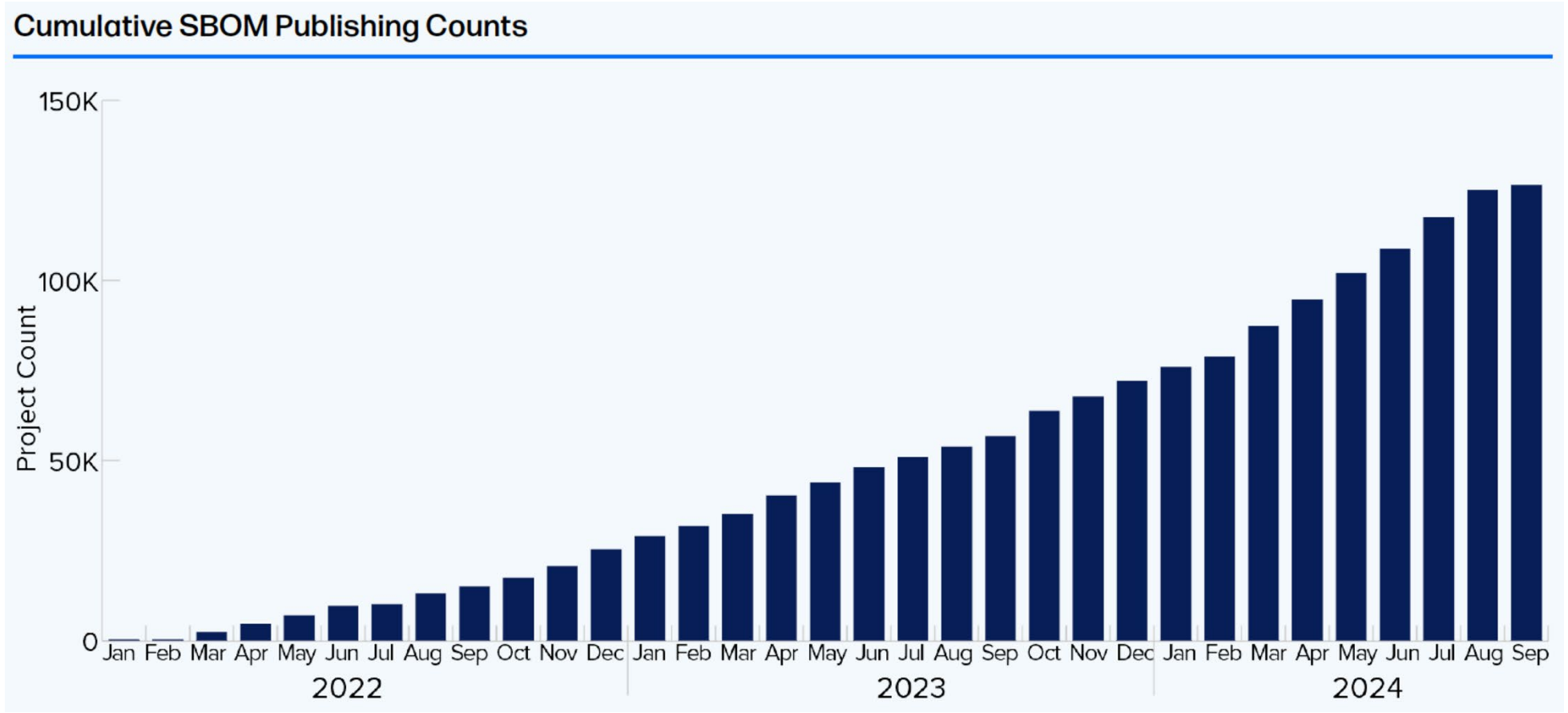
Source: 10th State of the Software Supply Chain® A DECADE OF DATA sonatype®

Backlog of Latent Security Vulnerabilities


PERSISTENT RISK AND CONSUMER COMPLACENCY BY THE NUMBERS
13%
Log4j downloads remain vulnerable 3 years after Log4shell exposure
ONLY 0.5%
OSS components have no available update.
NEARLY ALL RISK IS PREVENTABLE
80%
application dependencies remain un-upgraded for over a year
3.6%
dependencies are upgraded to another insecure version, so are still vulnerable

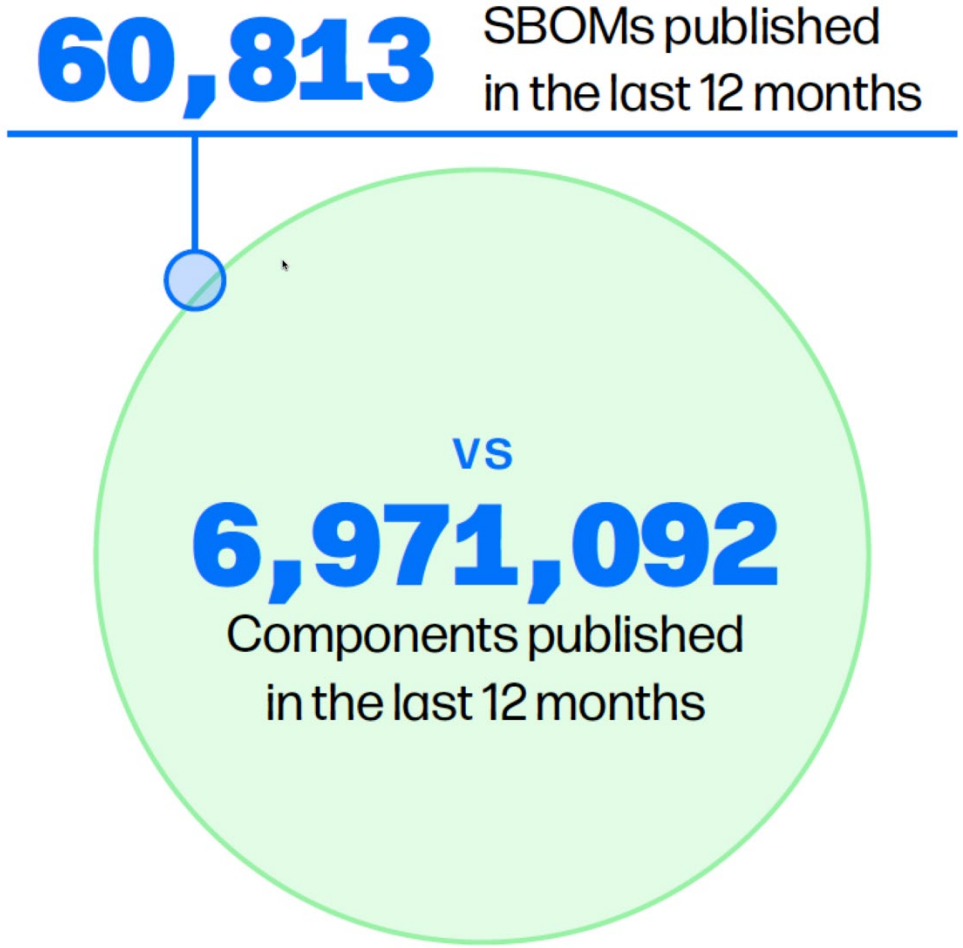
Source: 10 State of the Software Supply Chain® A DECADE OF DATA sonatype

Backlog of Latent Security Vulnerabilities

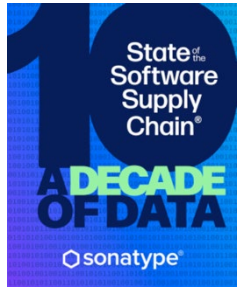

Cumulative SBOM Publishing Counts
150K
100K
50K
0
Project Count
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep
2022
2023
2024

Source: 10 State of the Software Supply Chain® A DECADE OF DATA sonatype®

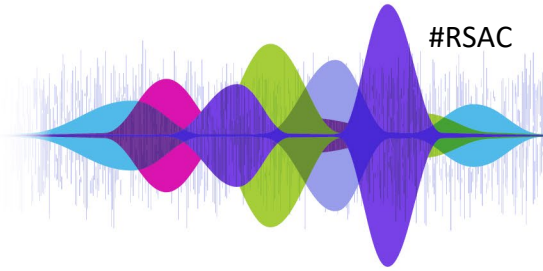
Disparity In Software Transparency & Traceability



Source:



New Methods of Software Creation



Innovations in the approach to developing software, such as today's **AI-first and vibe coding movements, are ushering in the greatest changes in how software is created**.

Like DevOps transformed software workflows across teams, cloud-native microservices changed software architecture, and Kubernetes transformed distributed workloads across applications and vendor offerings, **new forms of software development will emerge to become the next commonly adopted practice for developing software and AI agents.**

Source: Who Wins the Agentic AI Software Development Race?, Futurum Intelligence, 2025

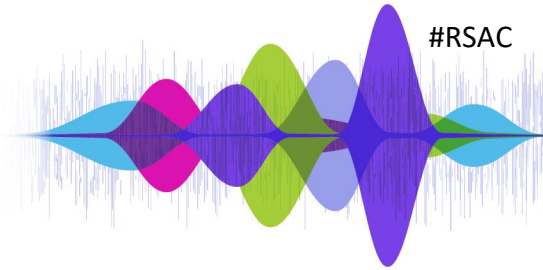
RSAC 2025 Conference

Key Questions

Software Supply Chain Security, AI, and Regulation

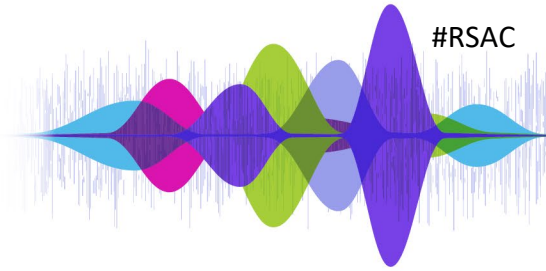
Many Voices.
One Community.

Key Questions



That’s how we are using AI. What about the AI models being embedded in their applications?

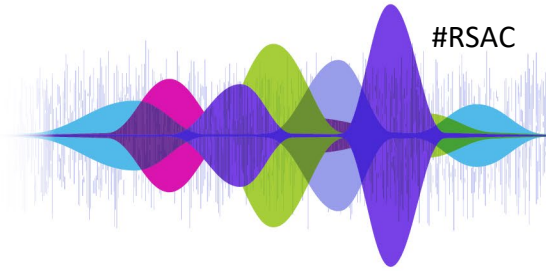
Key Questions



Where do AI models and agents (and their sources) fall into the software supply chain?

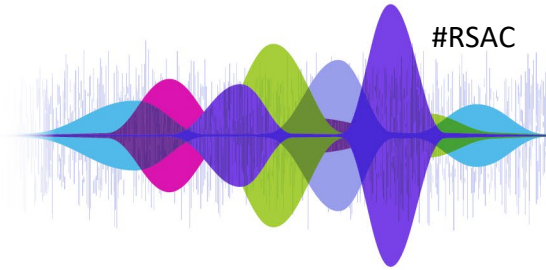
(And…how do we secure them?)

Key Questions

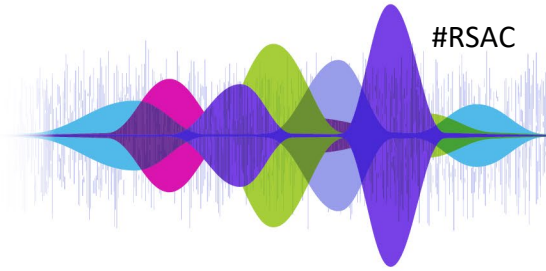


What is the role of SBOMs and Software Composition Analysis (SCA) with AI, models, and agents?

Key Questions



What is on the regulatory front and how will it drive security accountability into software and AI?



Q & A

The “Apply” Slide

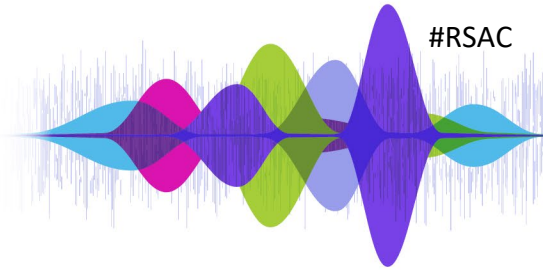
- Redefine your software supply chain incorporate incorporating AI:
  - AI/ML/GenAI models, code, and data
  - AI repositories, libraries, and data
    - Hugging Face*, TensorFlow Hub, PyTorch Hub, GitHub*, OpenVINO Model Zoo*, Kaggle*, ONNX Model Zoo*, H2O.ai, Scikit-learn, OpenCV, GGUF, and more

      * Data download available

  - SBOMs for AI systems (AIBOM, MLBOM)
    - The AI model itself (including its version, dependencies, and provenance)
    - The datasets used for training and testing the model

- Resources: Futurum Research Reports (https://futurumgroup.com/research-reports/)

“Apply” – Sources of AI Models & Data



- Hugging Face: You can download both AI models and datasets (including test data) from Hugging Face. The platform provides multiple methods for downloading models, such as using the `huggingface_hub` Python library, command-line tools, or Git, and datasets can be accessed similarly.
- TensorFlow Hub: This is a repository of trained machine learning models that are ready for download, fine-tuning, and deployment. You can directly load models into your TensorFlow projects.
- PyTorch Hub: PyTorch Hub allows you to list, download, and load pre-trained models for use in PyTorch projects directly from the repository.
- ONNX Model Zoo: The ONNX Model Zoo is a curated collection of pre-trained models in the ONNX format. You can download models and associated test data for validation and inference.
- OpenVINO Open Model Zoo: This repository includes optimized, pre-trained deep learning models and demos. Models can be downloaded and used for development and deployment with the OpenVINO toolkit.
- GitHub: Many researchers and organizations publish models and datasets on GitHub. GitHub also provides an interface called “GitHub Models” where you can find, experiment with, and download AI models for prototyping and production use.
- Kaggle: Kaggle is a leading source for datasets, including test data, used in data science and machine learning projects. Datasets can be downloaded manually or using the Kaggle API for use in your own projects.
- H2O.ai: H2O provides tools to build, save, and download machine learning models (including binary and MOJO formats) for local use or deployment.
- GGUF (GGML-based models): GGUF is a binary format for storing and distributing AI models, particularly for use with GGML-based executors. Models are typically developed in frameworks like PyTorch and then converted to GGUF for fast loading and inference

RSAC™ 2025 Conference

Many Voices.
One Community.

mashley@futurumgroup.com

twarden@sonatype.com